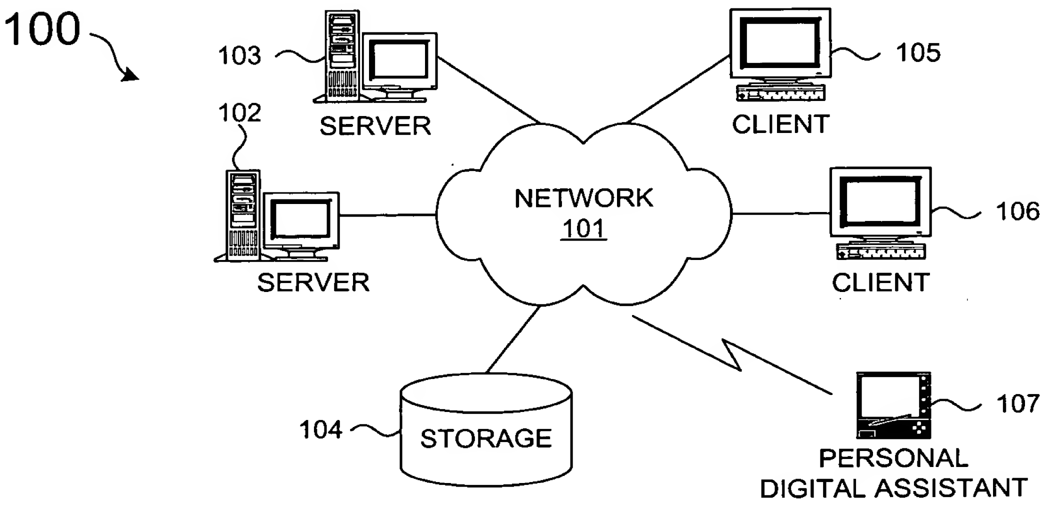

FIG. 1A
(PRIOR ART)

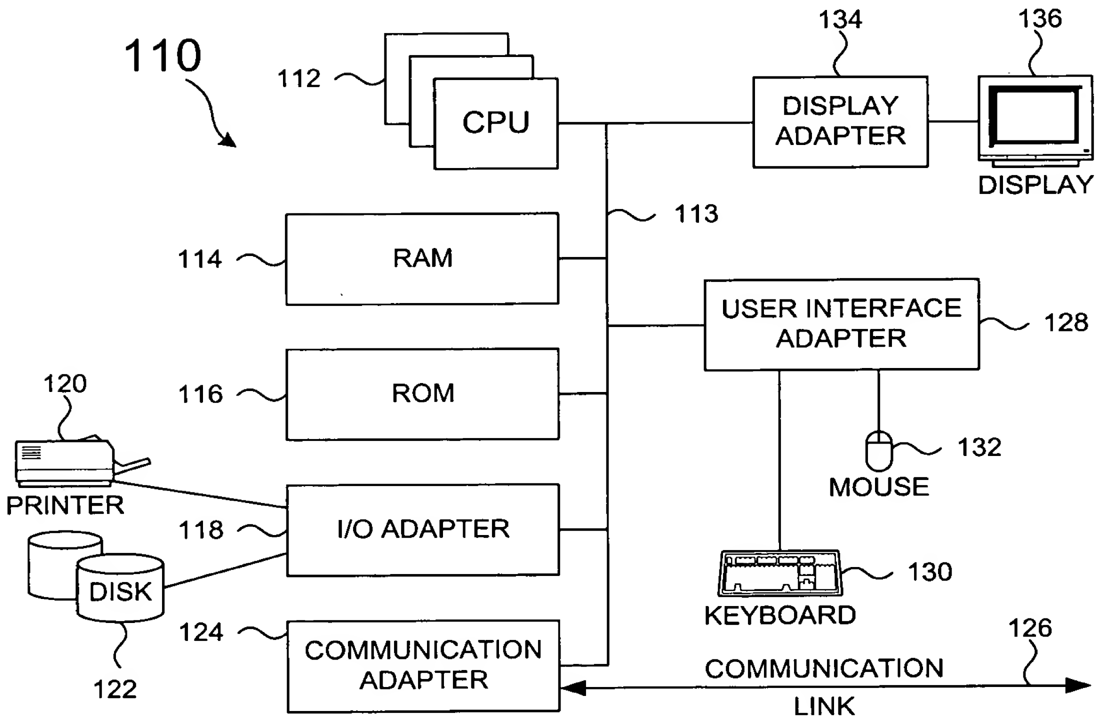

FIG. 1B
(PRIOR ART)

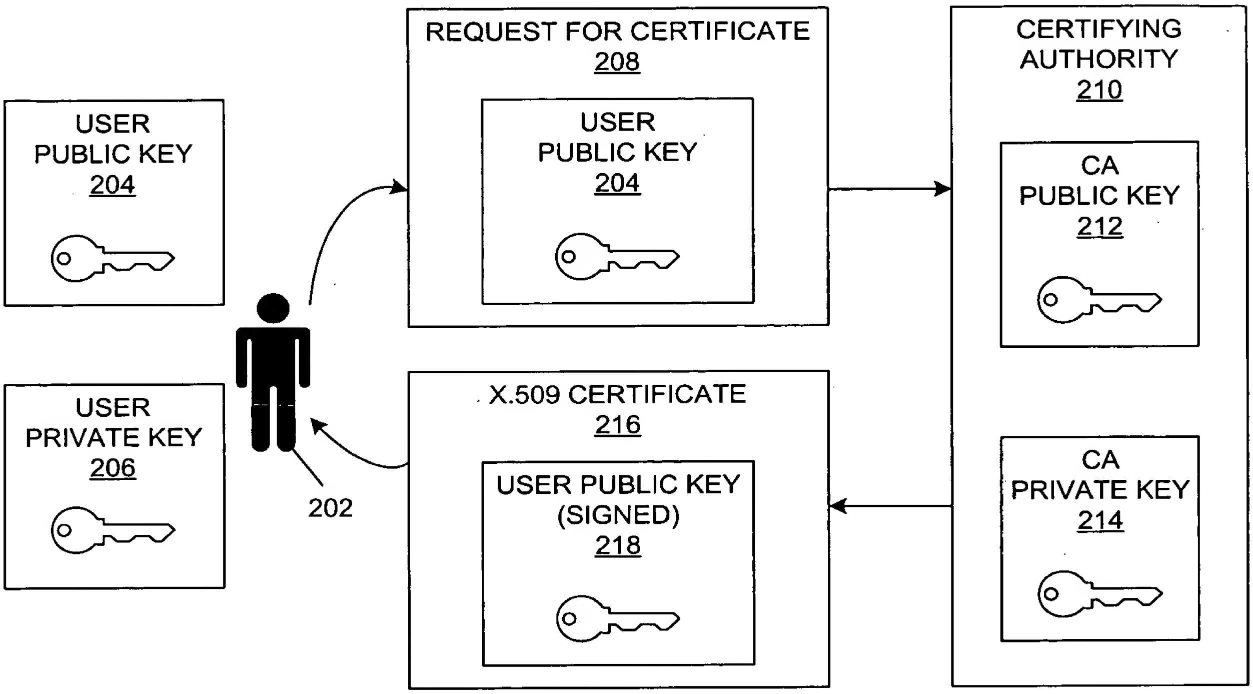

FIG. 2
(PRIOR ART)

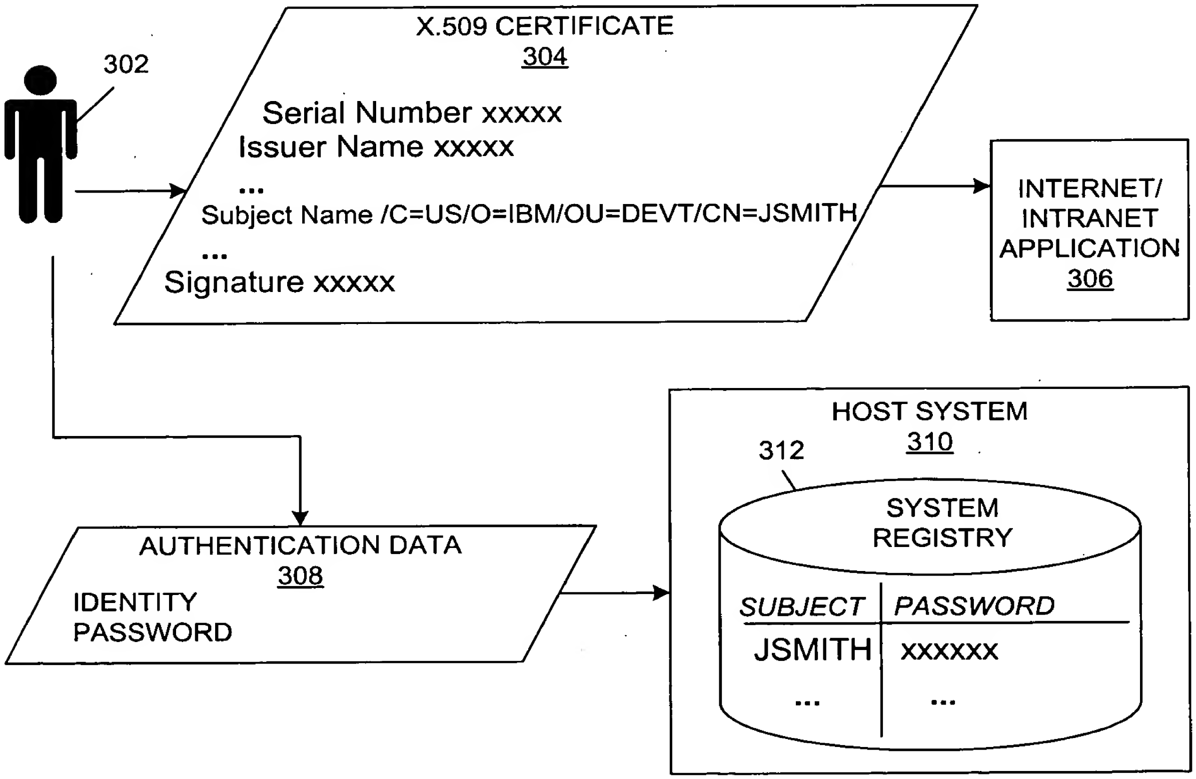

FIG. 3

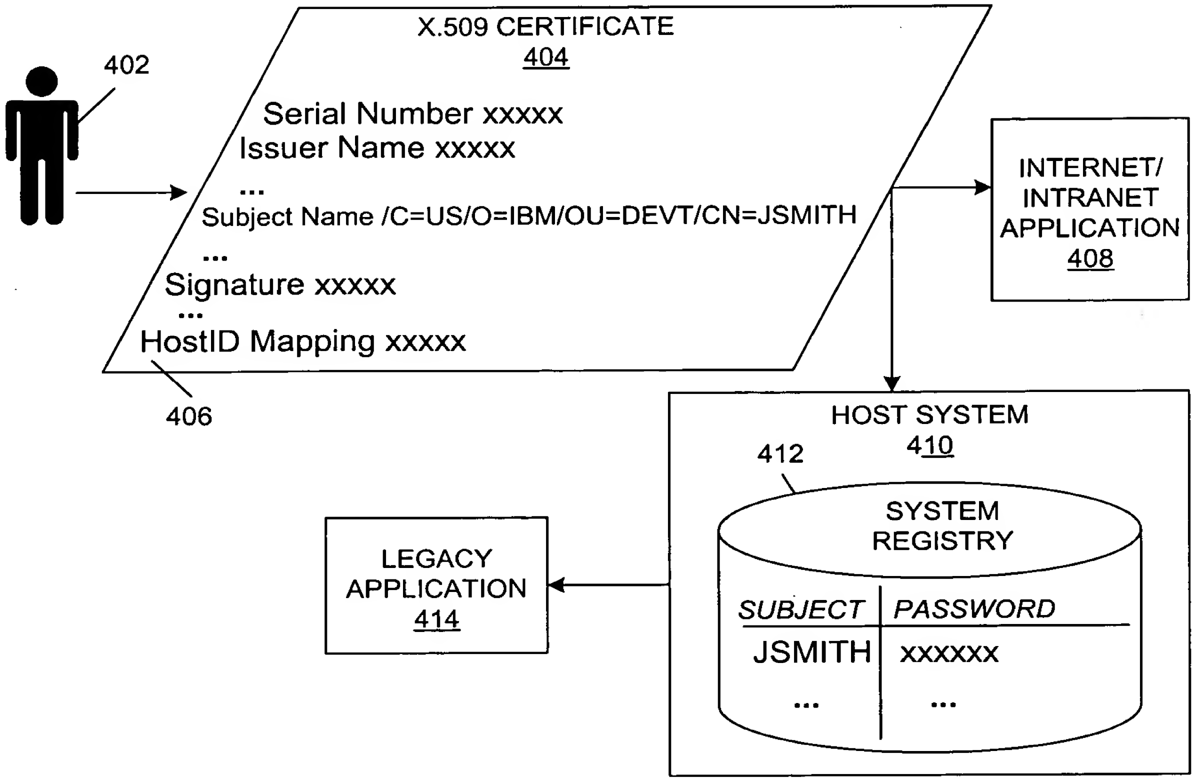

FIG. 4

```
HostIdMapping   ::=  SEQUENCE   {
     hostName           [1]  IMPLICIT  IA5String,
     subjectID               IMPLICIT  IA5String,
     proofOfIdPossession               IdProof OPTIONAL  }

IdProof   ::=  SEQUENCE   {
     secret                  OCTET STRING,
     encryptionAlgorithm     OBJECT IDENTIFIER   }
```

FIG. 6

```
Certificate  ::=  SEQUENCE  {
      tbsCertificate          TBSCertificate,
      signatureAlgorithm      AlgorithmIdentifier,
      signature               BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
      version            [0]  Version DEFAULT v1,
      serialNumber            CertificateSerialNumber,
      signature               AlgorithmIdentifier,
      issuer                  Name,
      validity                Validity,
      subject                 Name,
      subjectPublicKeyInfo    SubjectPublicKeyInfo,
      issuerUniqueID     [1]  IMPLICIT UniqueIdentifier OPTIONAL,
      subjectUniqueID    [2]  IMPLICIT UniqueIdentifier OPTIONAL,
      extensions         [3]  Extensions OPTIONAL   }

Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }

CertificateSerialNumber  ::=  INTEGER

Validity ::= SEQUENCE {
      notBefore               Time,
      notAfter                Time }

Time ::= CHOICE {
      utcTime                 UTCTime,
      generalTime             GeneralizedTime }

UniqueIdentifier  ::=  BIT STRING

SubjectPublicKeyInfo  ::=  SEQUENCE  {
      algorithm               AlgorithmIdentifier,
      subjectPublicKey        BIT STRING  }

Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
      extnID                  OBJECT IDENTIFIER,
      critical                BOOLEAN DEFAULT FALSE,
      extnValue               OCTET STRING  }
```

FIG. 5
(PRIOR ART)

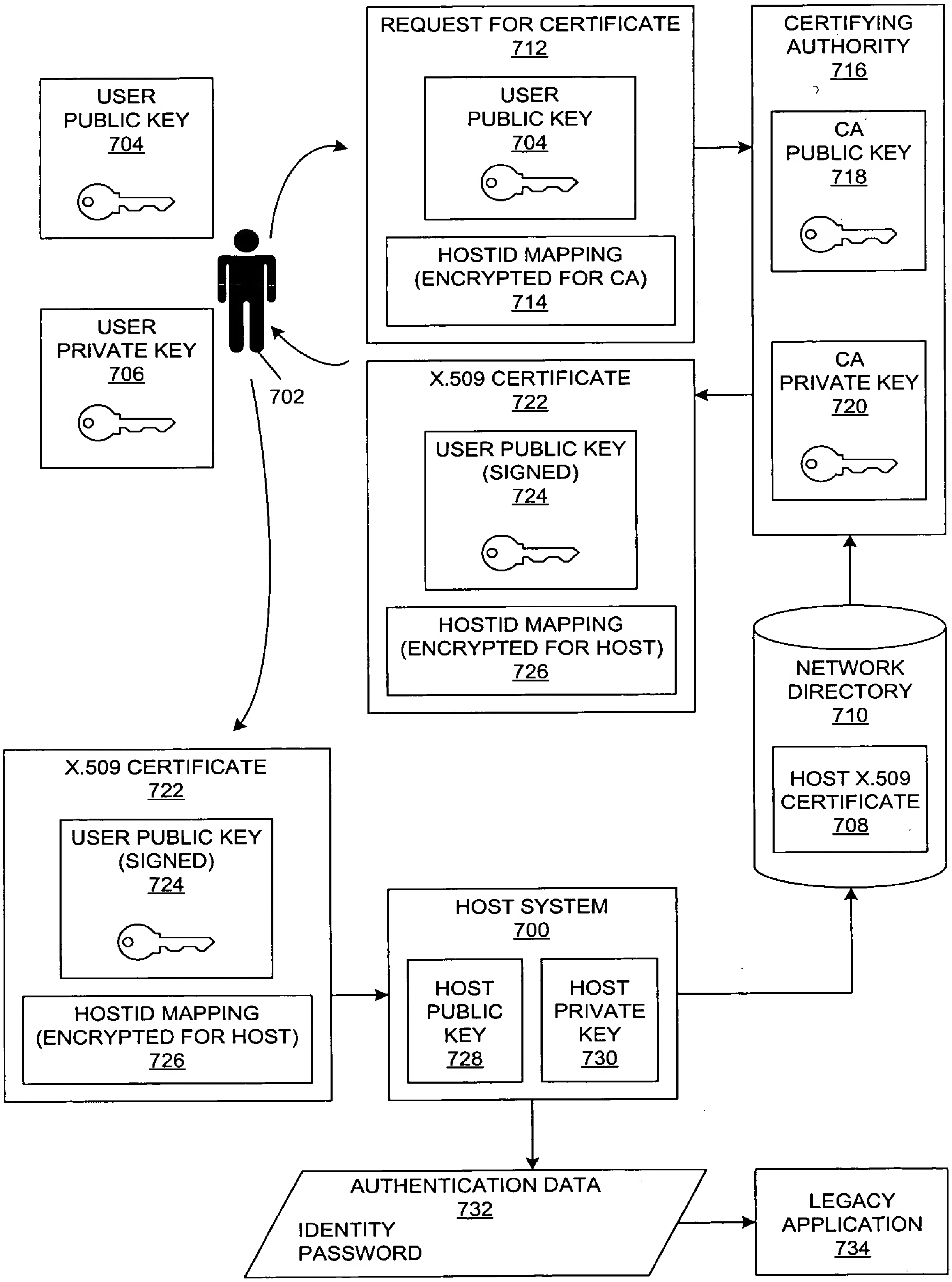
USER PUBLIC KEY 704
USER PRIVATE KEY 706
702
REQUEST FOR CERTIFICATE 712
USER PUBLIC KEY 704
HOSTID MAPPING (ENCRYPTED FOR CA) 714
CERTIFYING AUTHORITY 716
CA PUBLIC KEY 718
CA PRIVATE KEY 720
X.509 CERTIFICATE 722
USER PUBLIC KEY (SIGNED) 724
HOSTID MAPPING (ENCRYPTED FOR HOST) 726
NETWORK DIRECTORY 710
HOST X.509 CERTIFICATE 708
X.509 CERTIFICATE 722
USER PUBLIC KEY (SIGNED) 724
HOSTID MAPPING (ENCRYPTED FOR HOST) 726
HOST SYSTEM 700
HOST PUBLIC KEY 728
HOST PRIVATE KEY 730
AUTHENTICATION DATA 732
IDENTITY
PASSWORD
LEGACY APPLICATION 734

FIG. 7

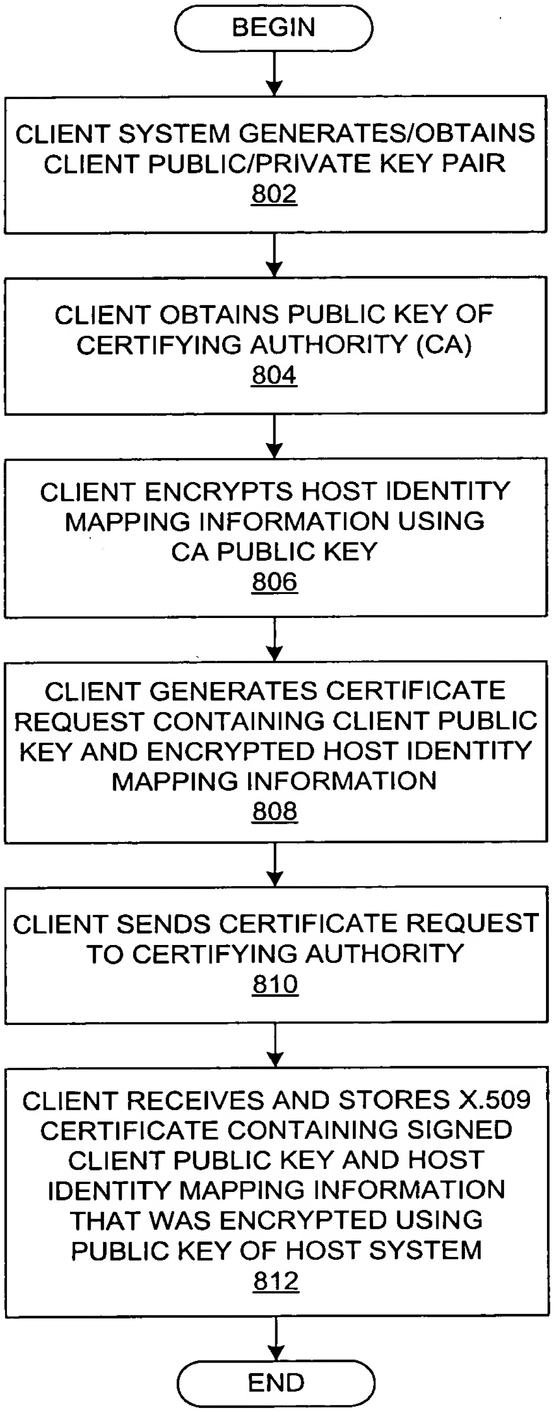
BEGIN
CLIENT SYSTEM GENERATES/OBTAINS CLIENT PUBLIC/PRIVATE KEY PAIR
802
CLIENT OBTAINS PUBLIC KEY OF CERTIFYING AUTHORITY (CA)
804
CLIENT ENCRYPTS HOST IDENTITY MAPPING INFORMATION USING CA PUBLIC KEY
806
CLIENT GENERATES CERTIFICATE REQUEST CONTAINING CLIENT PUBLIC KEY AND ENCRYPTED HOST IDENTITY MAPPING INFORMATION
808
CLIENT SENDS CERTIFICATE REQUEST TO CERTIFYING AUTHORITY
810
CLIENT RECEIVES AND STORES X.509 CERTIFICATE CONTAINING SIGNED CLIENT PUBLIC KEY AND HOST IDENTITY MAPPING INFORMATION THAT WAS ENCRYPTED USING PUBLIC KEY OF HOST SYSTEM
812
END

FIG. 8A

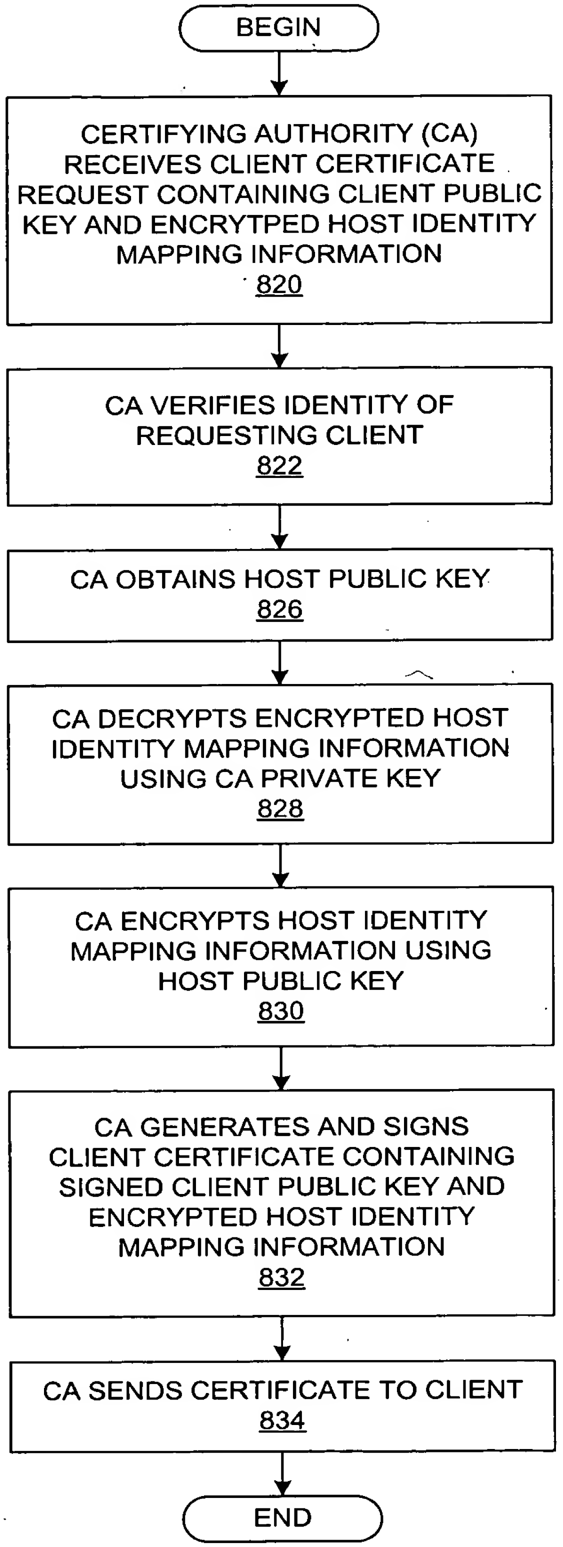
BEGIN
CERTIFYING AUTHORITY (CA) RECEIVES CLIENT CERTIFICATE REQUEST CONTAINING CLIENT PUBLIC KEY AND ENCRYTPED HOST IDENTITY MAPPING INFORMATION
820
CA VERIFIES IDENTITY OF REQUESTING CLIENT
822
CA OBTAINS HOST PUBLIC KEY
826
CA DECRYPTS ENCRYPTED HOST IDENTITY MAPPING INFORMATION USING CA PRIVATE KEY
828
CA ENCRYPTS HOST IDENTITY MAPPING INFORMATION USING HOST PUBLIC KEY
830
CA GENERATES AND SIGNS CLIENT CERTIFICATE CONTAINING SIGNED CLIENT PUBLIC KEY AND ENCRYPTED HOST IDENTITY MAPPING INFORMATION
832
CA SENDS CERTIFICATE TO CLIENT
834
END

FIG. 8B

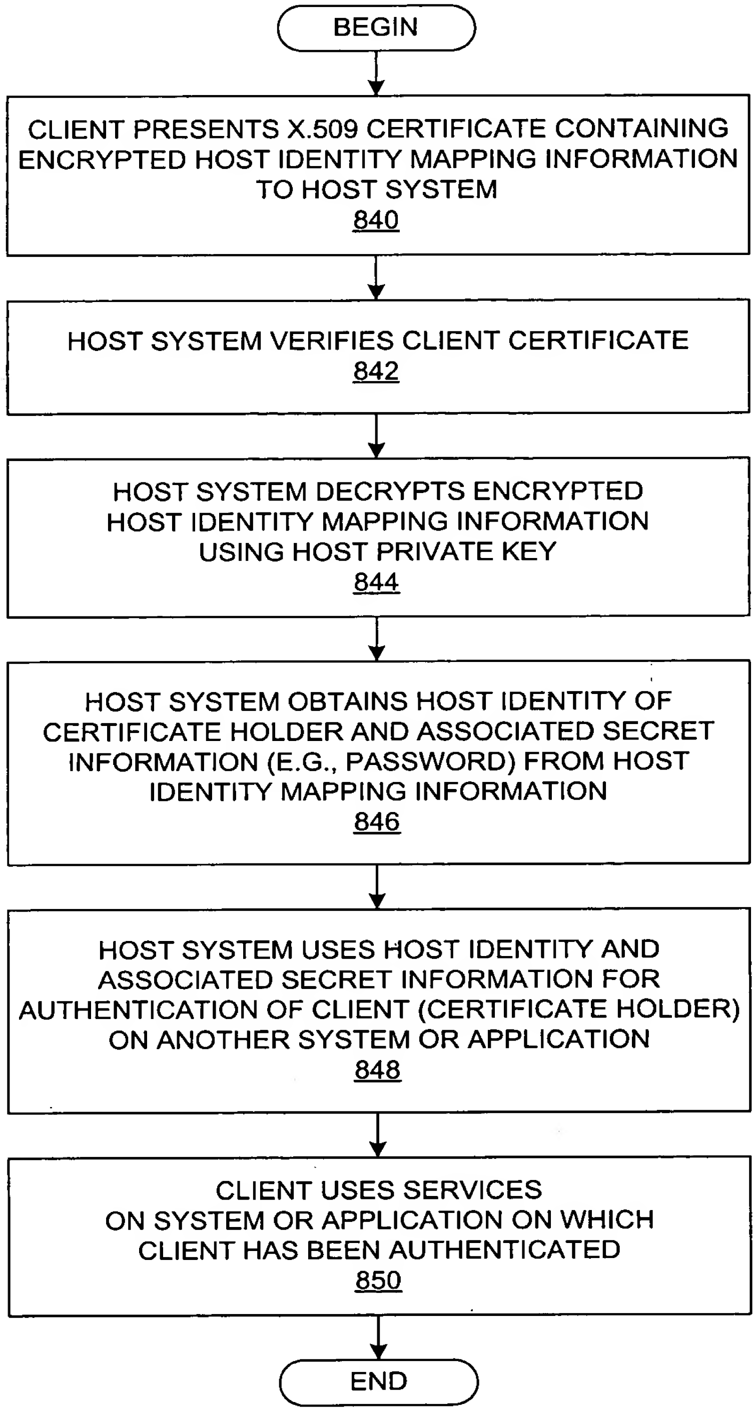
BEGIN
CLIENT PRESENTS X.509 CERTIFICATE CONTAINING ENCRYPTED HOST IDENTITY MAPPING INFORMATION TO HOST SYSTEM
840
HOST SYSTEM VERIFIES CLIENT CERTIFICATE
842
HOST SYSTEM DECRYPTS ENCRYPTED HOST IDENTITY MAPPING INFORMATION USING HOST PRIVATE KEY
844
HOST SYSTEM OBTAINS HOST IDENTITY OF CERTIFICATE HOLDER AND ASSOCIATED SECRET INFORMATION (E.G., PASSWORD) FROM HOST IDENTITY MAPPING INFORMATION
846
HOST SYSTEM USES HOST IDENTITY AND ASSOCIATED SECRET INFORMATION FOR AUTHENTICATION OF CLIENT (CERTIFICATE HOLDER) ON ANOTHER SYSTEM OR APPLICATION
848
CLIENT USES SERVICES ON SYSTEM OR APPLICATION ON WHICH CLIENT HAS BEEN AUTHENTICATED
850
END

FIG. 8C